IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MICHIGAN

TOMMIE TIPTON, *individually and on behalf of all others similarly situated*, Plaintiff, v. VPS OF MI, PLLC, Defendant.	Case No.: _____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff, Tommie Tipton ("Plaintiff"), individually and on behalf of the Class defined below of similarly situated persons, alleges the following against Defendant, VPS of MI, PLLC ("VPS" or "Defendant"), based upon personal knowledge with respect to himself and on information and belief derived from, among other things, investigation by counsel as to all other matters:

SUMMARY OF THE CASE

1. This action arises from VPS's failure to secure the protected health

information ("PHI")[1] and personally identifiable information ("PII")[2] (collectively "Private Information") of Plaintiff and the members of the proposed Class, where VPS provided healthcare services to Plaintiff and Class members.

2. VPS "is a group of Board Certified Healthcare Professionals whose primary focus is to provide caring, compassionate and quality in-home physician services for homebound Michiganders."[3]

3. On or about June 4, 2024, VPS discovered an unauthorized actor obtained Plaintiff's and Class Members' Private Information from VPS's computer

[1] Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. "Business Health information such as diagnoses, treatment information, medical test results, and prescription information are considered protected health information under HIPAA, as are national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information. *Summary of the HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html (last visited Nov. 26, 2024).

[2] The Federal Trade Commission defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." 17 C.F.R. § 248.201(b)(8).

[3] https://vpsofmi.com/ (last visited Nov. 26, 2024).

systems (the "Data Breach").[4]

4. The Private Information that intruders accessed and infiltrated from VPS's systems included for patients included, but is not limited to, full names, Social Security numbers, driver's license numbers, medical history information, mental or physical condition or diagnosis, medical treatment information, disability information, prescription information, medical record numbers, health insurance policy numbers, subscriber numbers, medical information, claims history, health insurance group or plan numbers.[5]

5. As a result of the Data Breach, which VPS failed to prevent, the Private Information of current and former patients, including Plaintiff and the proposed Class Members, was stolen.[6]

6. Among myriad industry standards and statutes for protection of sensitive information, PHI is specifically governed by federal law under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and its implementing regulations. HIPAA requires entities like VPS to take appropriate technical, physical, and administrative safeguards to secure the privacy of PHI,

[4] *See* Notice Letter, a sample copy, is available at https://ago.vermont.gov/sites/ago/files/documents/2024-11-15%20VPS%20of%20MI.%20Data%20Breach%20Notice%20to%20Consumers.pdf (last viewed Dec. 3, 2024).
[5] *See id.*
[6] *See id*.

establishes national standards to protect PHI, and requires timely notice of a breach of unencrypted PHI.

7. Instead, VPS disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, and/or negligently failing to implement reasonable measures to safeguard its patients' Private Information and by failing to take necessary steps to prevent unauthorized disclosure of that information. VPS's woefully inadequate data security measures made the Data Breach a foreseeable, and even likely, consequence of its negligence.

8. Further exacerbating Plaintiff's injuries, VPS has offered insufficient assurances that all personal data or copies of data have been recovered or destroyed, or that VPS has adequately enhanced its security practices or dedicated sufficient resources and staff to avoid a similar breach of its network in the future.

9. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have suffered actual and present injuries, including but not limited to: (a) present, certainly impending, and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; (b) diminution of value of their Private Information; (c) loss of benefit of the bargain (price premium damages); (d) loss of value of privacy and confidentiality of the stolen Private Information; (e) illegal sales of the compromised Private Information; (f) mitigation expenses and time spent responding to and remedying the effects of the Data Breach; (g) identity

theft insurance costs; (h) "out of pocket" costs incurred due to actual identity theft; (i) credit freezes/unfreezes; (j) expense and time spent on initiating fraud alerts and contacting third parties; (k) decreased credit scores; (l) lost work time; (m) anxiety, annoyance, and nuisance; (n) continued risk to their Private Information, which remains in VPSs possession and is subject to further breaches so long as VPS fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information; and (o) disgorgement damages associated with VPS's maintenance and use of Plaintiff's data for its benefit and profit..

10. Plaintiff and Class Members would not have provided their valuable Private Information to VPS had they known that VPS would make their Private Information Internet-accessible, not encrypt personal and sensitive data elements and not delete the Private Information it no longer had reason to maintain.

11. Through this lawsuit, Plaintiff seek to hold VPS responsible for the injuries it inflicted on Plaintiff and Class Members due to its impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information that remains in VPS's possession.

JURISDICTION AND VENUE

12. This Court has subject matter jurisdiction over this action under 28 U.S.C.§ 1332(d) because this is a class action wherein the amount in controversy

exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.[7]

13. This Court has personal jurisdiction over Defendant because its principal place of business is in this District, regularly conducts business in Michigan, transacted business with Plaintiff and Class Members within Michigan, entered into contracts with Plaintiff and Class Members in Michigan, and the acts and omissions giving rise to Plaintiff's claims occurred in and emanated from this District.

14. Venue is proper under 18 U.S.C § 1391(b)(1) because Defendant's headquarters and principal place of business is in this District.

PARTIES

15. Plaintiff Tommie Tipton is, and at all relevant times has been, a resident and citizen of Dearborn Heights, Michigan, where he intends to remain.

16. Defendant VPS is a limited liability company incorporated under the laws of Michigan with its headquarters and principal place of business located at 31500 West 13 Mile Road, Suite 100, Farmington Hills, Michigan 48334.

[7] According to a sample notice released by the Office of the Attorney General in Vermont, residents of at least Vermont, Maryland, North Carolina, and New York appear to have been impacted by the Data Breach. *See* Notice Letter, n.4.

FACTUAL ALLEGATIONS

A. The VPS Data Breach

17. VPS provides a wide variety of medical care for adults and children across the state of Michigan.

18. In the ordinary course of receiving health care services from Defendant VPS, each patient must provide (and Plaintiff did provide) Defendant VPS with sensitive, personal, and private information, as part of the healthcare professional-patient relationship, and as a condition of receiving services.

19. On or about June 4, 2024, Plaintiff's and Class Members' Private Information in possession of VPS was obtained by an unauthorized party, which VPS describes in its Notice Letter.[8]

20. Approximately eight months later, on November 15, 2024, VPS began sending out Notice Letters to affected persons, informing them that their Private Information had been compromised in the Data Breach:

> **What Happened?**
>
> On June 4, 2024, VPS detected irregular activity within our computer network. VPS launched an investigation and determined that our server had been infected with malware, which prevented access to certain files on our server. Through our investigation we also determined that an unauthorized actor exfiltrated information from our server.

[8] *See* Notice Letter, n.4.

What Information Was Involved?

> The following information was potentially exfiltrated from our network, if you supplied it to VPS: your name, Social Security number, and/or driver's license number. In addition, the following medical information was potentially exfiltrated, if part of your VPS medical record: medical history information, mental or physical condition or diagnosis by a health care professional, medical treatment information, disability information, prescription information, and medical record number. If part of our records, the following information related to your health insurance was also potentially exfiltrated: health insurance policy number; subscriber number; any medical information in an individual's health insurance application and claims history, including any appeals records; and health insurance group or plan number.[9]

21. Upon information and belief, the cyberattack was targeted at Defendant, due to its status as a healthcare provider that collects, creates, and maintains Private Information on its computer networks and/or systems.

22. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, causing the exposure of Private Information.

23. The attacker accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including, name, address, Social Security Number, and medical information.

[9] *See id*.

Plaintiff's and Class Members' Private Information was accessed and stolen in the Data Breach.

24. As evidenced by the Data Breach, the Private Information contained in Defendant's network was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

B. The Value of Private Information

25. In April 2020, ZDNet reported in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year", that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for complaints as revenge against those who refuse to pay."[10]

26. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[11]

[10] https://www.zdnet.com/article/ransomeware-mentioned-in-1000-sec-filings-over-the-past-year/ (last visited Nov. 26, 2024).
[11] *See* https://www.cisa.gov/sites/default/files/2023-01-CISA_MSISAC_Ransomware%20Guide_ 8508C.pdf (last visited Nov. 26, 2024).

27. Stolen Private Information is often trafficked on the dark web, as is the case here. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

28. When malicious actors infiltrate companies and copy and exfiltrate the PII that those companies store, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.[12]

29. Another example is when the U.S. Department of Justice announced its seizure of AlphaBay in 2017, AlphaBay had more than 350,000 listings, many of which concerned stolen or fraudulent documents that could be used to assume another person's identity. Other marketplaces, similar to the now-defunct AlphaBay, "are awash with [PII] belonging to victims from countries all over the world. One of the key challenges of protecting PII online is its pervasiveness. As data breaches in the news continue to show, PII about employees, customers and the public is housed in all kinds of organizations, and the increasing digital transformation of today's businesses only broadens the number of potential sources for hackers to target."[13]

[12] *Shining a Light on the Dark Web with Identity Monitoring, IdentityForce*, Dec. 28, 2020, https://www.identityforce.com/blog/shining-light-dark-web-identity-monitoring (last visited Nov. 26, 2024).
[13] *Stolen PII & Ramifications: Identity Theft and Fraud on the Dark Web*, Armor, April 3, 2018, https://www.armor.com/resources/blog/stolen-pii- ramifications-identity-theft-fraud-dark-web/ (last visited Nov. 26, 2024).

30. The Private Information of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, Private Information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $2009.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[15] Criminals can also purchase access to entire company data breaches.[16]

31. In addition, due to the highly valuable nature of PHI, the FBI has warned healthcare providers that they are likely to be the targets of cyberattacks like the one at issue here.[17]

32. Once Private Information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional PII being harvested from the

[14] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal- data-sold-on-the-dark-web- how-much-it-costs/ (last visited Nov. 26, 2024).
[15] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is- selling-for-on-the-dark-web/ (last visited Nov. 26, 2024).
[16] *In the Dark*, VPNOverview, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the- dark/ (last visited Nov. 26, 2024).
[17] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS (Aug. 20, 2014), https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK2 4U20140820.

victim, as well as PII from family, friends and colleagues of the original victim.

33. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses in 2019, resulting in more than $3.5 billion in losses to individuals and business victims.

34. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

35. Data breaches facilitate identity theft as hackers obtain consumers' Private Information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' PII to others who do the same.

36. For example, the United States Government Accountability Office noted in a June 2007 report on data breaches (the "GAO Report") that criminals use Private Information to open financial accounts, receive government benefits, and make purchases and secure credit in a victim's name.[18] The GAO Report further notes that this type of identity fraud is the most harmful because it may take some

[18] *See* Government Accountability Office, *Personal Information: Data Breaches are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown* (June 2007), https://www.gao.gov/assets/gao- 07-737.pdf (last visited Nov. 26, 2024).

time for a victim to become aware of the fraud, and can adversely impact the victim's credit rating in the meantime. The GAO Report also states that identity theft victims will face "substantial costs and inconveniences repairing damage to their credit records . . . [and their] good name."[19]

37. The market for Private Information has continued unabated to the present, and in 2023 the number of reported data breaches in the United States increased by 78% over 2022, reaching 3205 data breaches.[20]

38. The exposure of Plaintiff's and Class Members' Private Information to cybercriminals will continue to cause substantial risk of future harm (including identity theft) that is continuing and imminent in light of the many different avenues of fraud and identity theft utilized by third-party cybercriminals to profit off of this highly sensitive information.

C. Healthcare Organizations are Prime Targets for Cyberattacks.

39. Healthcare organizations are prime targets for cyberattacks because of the information they collect and store, including financial information of patients, login credentials, insurance information, medical records and diagnoses, and

[19] *Id*.

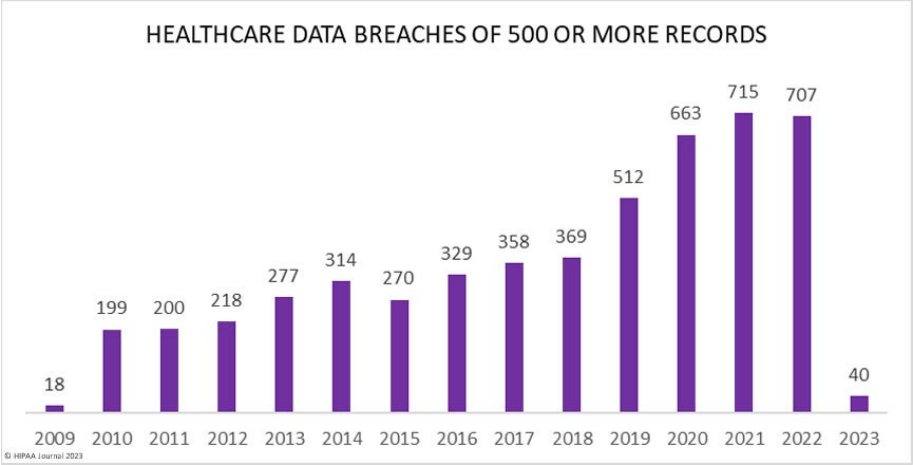
[20] Beth Maundrill, *Data Privacy Week: US Data Breaches Surge, 2023 Sees 78% Increase in Compromises*, INFOSECURITY MAGAZINE (Jan. 23, 2024); https://www.infosecurity-magazine.com/news/us-data-breaches-surge-2023/ (last visited Nov. 26, 2024); *see also* Identity Theft Resource Center, *2023 Data Breach Report*, https://www.idtheftcenter.org/publication/ 2023-data-breach-report/ (last visited Nov. 26, 2024).

personal information of employees, customers and patients—all extremely valuable in underground markets.

40. This was known and obvious to VPS as they observed frequent public announcements of data breaches affecting the healthcare industry and knew that information of the type it collected, maintained, and stored is highly coveted and a frequent target of cybercriminals.

41. For example, a report by the HIPAA Journal noted that "Between 2009 and 2022, 5,150 healthcare data breaches of 500 or more records have been reported to the HHS' Office for Civil Rights. Those breaches have resulted in the exposure or impermissible disclosure of 382,262,109 healthcare records. That equates to more than 1.2X the population of the United States. In 2018, healthcare data breaches of 500 or more records were being reported at a rate of around 1 per day. Fast forward 5 years and the rate has more than doubled. In 2022, an average of 1.94 healthcare data breaches of 500 or more records were reported each day."[21]

[21] https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited Nov. 26, 2024).



42. Ransomware attacks are especially prevalent in the industry. For years federal agencies have warned about the increasing risk of ransomware attacks on companies holding PII and PHI. For example, in October 2019 the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."[22]

43. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims

[22] https://www.ic3.gov/Media/Y2019/PSA191002 (last visited Nov. 26, 2024).

for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion."[23]

44. In March 2021, Tenable Security Response Team conducted a root cause analysis of 293 healthcare breaches known to have exposed records between January 2020 and February 2021, and concluded that "ransomware was by far the most prominent root case of healthcare breaches, accounting for a whopping 54.95%."[24]

45. At all relevant times, VPS knew, or reasonably should have known, of the importance of safeguarding Private Information and the foreseeable consequences that would occur if its data security systems were breached, including, specifically, the significant costs that would be imposed on affected individuals as a result of the breach.

46. VPS was, or should have been, fully aware of the significant number of individuals whose Private Information it collected and stored, thus, the significant number of individuals who would be harmed by a breach of VPS's systems.

[23] https://www.cisa.gov/stopransomware/ransomware-faqs#:~:text=Malicious%20actors%20continue%20to%20adjust,as%20secondary%20forms%20of%20extortion (last visited Nov. 26, 2024).
[24] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last visited Nov. 26, 2024).

47. Despite all the publicly available knowledge of the serious threat of compromises of personal information and despite holding the Private Information of millions of individuals, VPS failed to use reasonable care in maintaining the privacy and security of Plaintiff's and Class Members' Private Information. Had VPS implemented adequate security measures, cybercriminals never could have accessed millions of individuals' files and the Data Breach would have been prevented or much smaller in scope.

D. VPS Failed to Comply with Regulatory Requirements and Standards.

48. Federal and state regulators have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and the healthcare sector. There are a number of state and federal laws, requirements, and industry standards governing the protection of Private Information.

49. For example, at least 24 states have enacted laws addressing data security practices that require businesses that own, license, or maintain Private Information about a resident of that state to implement and maintain "reasonable security procedures and practices" and to protect Private Information from unauthorized access.

50. Additionally, cybersecurity firms have promulgated a series of best practices that at a minimum should be implemented by sector participants including,

but not limited to: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting of physical security systems; protecting against any possible communication system; and training staff regarding critical points.[25]

51. The FTC has issued several guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be considered for all business decision-making.[26]

52. Under the FTC's 2016 *Protecting Personal Information: Guide for Business* publication, the FTC notes that businesses should safeguard the personal customer information they retain; properly dispose of unnecessary personal information; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to rectify security issues.[27]

53. The guidelines also suggest that businesses use an intrusion detection system to expose a breach as soon as it happens, monitor all incoming traffic for

[25] *See Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, INC. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security (last visited Nov. 26, 2024).
[26] *Start With Security*, Fed. Trade Comm'n ("FTC"), https://www.ftc.gov/system/files/ documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Nov. 26, 2024).
[27] *Protecting Personal Information: A Guide for Business*, FTC, https://www.ftc.gov/system/files/ documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Nov. 26, 2024).

activity indicating someone is trying to hack the system, watch for large amounts of data being siphoned from the system, and have a response plan in the event of a breach.

54. The FTC advises companies to not keep information for periods of time longer than needed to authorize a transaction, restrict access to private information, mandate complex passwords to be used on networks, utilize industry-standard methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[28]

55. The FTC has brought enforcement actions against companies for failing to adequately and reasonably protect consumer data, treating the failure to do so as an unfair act or practice barred by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders originating from these actions further elucidate the measures businesses must take to satisfy their data security obligations.

56. VPS's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

57. VPS's failure to verify that it had implemented reasonable security measures constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

[28] *Supra*, n.39.

58. Furthermore, VPS is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C. The Privacy Rule and the Security Rule set nationwide standards for protecting health information, including health information stored electronically.

59. The Security Rule requires VPS to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.[29]

60. Pursuant to HIPAA's mandate that VPS follow "applicable standards, implementation specifications, and requirements . . . with respect to electronic

[29] *Summary of the HIPAA Security Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html (last visited Nov. 26, 2024).

protected health information," 45 C.F.R. § 164.302, VPS was required to, at minimum, "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information," 45 C.F.R. § 164.306(e), and "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

61. VPS is also required to follow the regulations for safeguarding electronic medical information pursuant to the Health Information Technology Act ("HITECH"). *See* 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

62. Both HIPAA and HITECH obligate VPS to follow reasonable security standards, respond to, contain, and mitigate security violations, and to protect against disclosure of sensitive patient Private Information. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); 45 C.F.R. § 164.530(f); 42 U.S.C. § 17902.

63. As alleged in this Complaint, VPS has failed to comply with HIPAA and HITECH. It has failed to maintain adequate security practices, systems, and protocols to prevent data loss, failed to mitigate the risks of a data breach and loss of data, and failed to ensure the confidentiality and protection of PHI.

E. VPS Failed to Comply with Industry Practices.

64. Various cybersecurity industry best practices have been published and should be consulted as a go-to resource when developing an organization's cybersecurity standards. The Center for Internet Security ("CIS") promulgated its Critical Security Controls, which identify the most commonplace and essential cyber-attacks that affect businesses every day and proposes solutions to defend against those cyber-attacks.[30] All organizations collecting and handling Private Information, such as VPS, are strongly encouraged to follow these controls.

65. Further, the CIS Benchmarks are the overwhelming option of choice for auditors worldwide when advising organizations on the adoption of a secure build standard for any governance and security initiative, including PCI DSS, HIPAA, NIST 800-53, SOX, FISMA, ISO/IEC 27002, Graham Leach Bliley and ITIL.[31]

[30] Center for Internet Security, *Critical Security Controls*, at 1 (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Nov. 26, 2024).
[31] *See CIS Benchmarks FAQ*, Center for Internet Security, https://www.cisecurity.org/cis-benchmarks/cis-benchmarks-faq/ (last visited Nov. 26, 2024).

66. Cybersecurity experts normally have identified data management companies, like VPS as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect, use, and maintain.[32]

67. Several best practices have been identified that a minimum should be implemented by data management companies like VPS, including but not limited to securely configuring business software, managing access controls and vulnerabilities to networks, systems, and software, maintaining network infrastructure, defending networks, adopting data encryption while data is both in transit and at rest, and securing application software.[33]

68. Other best practices have been identified that a minimum should be implemented by companies like VPS using third-party providers, including but not limited to ensuring that Private Information is only shared with third parties when reasonably necessary and that those vendors have appropriate cybersecurity systems and protocols in place.[34]

---

[32] *See Security Questions to Ask After the ZeroedIn Breach*, Information Week, https://www.informationweek.com/cyber-resilience/security-questions-to-ask-after-the-zeroedin-breach (last visited Nov. 26, 2024) (commenting that the growing outsourcing of data analytics work to third-party service providers may offer to malicious cyber-attackers novel "targets of opportunity – breach one data manager and gain access to data from a multitude of sources.).

[33] *See* Center for Internet Security, *Critical Security Controls* (May 2021), https://learn.cisecurity.org/CIS-Controls-v8-guide-pdf (last visited Nov. 26, 2024).

[34] *See id*.

69. VPS failed to follow these and other industry standards to adequately protect the Private Information of Plaintiff and Class Members.

F. Defendant's Conduct Violated HIPPA

70. HIPAA requires covered entities such as Defendant to protect against reasonably anticipated threats to the security of sensitive patient health information.

71. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

72. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, et seq. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PII like the data Defendant left unguarded. The HHS subsequently promulgated multiple regulations under authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.306(a) (1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

73. A Data Breach such as the one Defendant experienced, is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "...the acquisition, access, use, or disclosure of PHI in a manner not

> permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

74. Defendant's Data Breach resulted from a combination of insufficiencies that demonstrate it failed to meet mandated by HIPAA regulations.

G. The Data Breach Caused Injury to Class Members and Will Result in Additional Harm Such as Fraud.

75. Without detailed disclosure to the victims of the Data Breach, individuals whose Private Information was compromised by the Data Breach, including Plaintiff and Class Members, were unknowingly and unwittingly exposed to continued misuse and ongoing risk of misuse of their Private Information for months without being able to take available precautions to prevent imminent harm.

76. The ramifications of VPS's failure to secure Plaintiff's and Class Members' data are severe.

77. Victims of data breaches are much more likely to become victims of identity theft and other types of fraudulent schemes. This conclusion is based on an analysis of four years of data that correlated each year's data breach victims with those who also reported being victims of identity fraud.

78. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC

[35] 17 C.F.R. § 248.201 (2013).

describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[36]

79. Identity thieves can use Private Information, such as that of Plaintiff and Class Members, which VPS failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as: immigration fraud; obtaining a driver's license or identification card in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

80. As demonstrated herein, these and other instances of fraudulent misuse of the compromised Private Information has already occurred and are likely to continue.

81. As a result of VPS's delay between the Data Breach in January and the notice of the Data Breach sent to affected persons in June, the risk of fraud for Plaintiff and Class Members increased exponentially.

82. Javelin Strategy and Research reported that identity thieves stole $112 billion from 2011 through 2016.[37]

---

[36] *Id.*

[37] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited Nov. 26, 2024).

83. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[38]

84. The 2017 Identity Theft Resource Center survey[39] evidences the emotional suffering experienced by victims of identity theft:

- 75% of respondents reported feeling severely distressed;
- 67% reported anxiety;
- 66% reported feelings of fear related to personal financial safety;
- 37% reported fearing for the financial safety of family members;
- 24% reported fear for their physical safety;
- 15.2% reported a relationship ended or was severely and negatively impacted by identity theft; and
- 7% reported feeling suicidal.

85. Identity theft can also exact a physical toll on its victims. The same survey reported that respondents experienced physical symptoms stemming from

[38] *Victims of Identity Theft*, Bureau of Justice Statistics (Sept. 2015) http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Nov. 26, 2024).
[39] *Id*.

their experience with identity theft:

- 48.3% of respondents reported sleep disturbances;
- 37.1% reported an inability to concentrate / lack of focus;
- 28.7% reported they were unable to go to work because of physical symptoms;
- 23.1% reported new physical illnesses (aches and pains, heart palpitations, sweating, stomach issues); and
- 12.6% reported a start or relapse into unhealthy or addictive behaviors.[40]

86. There may be a time lag between when harm occurs versus when it is discovered, and also between when private information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[41]

Thus, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights.

---

[40] *Id*.

[41] GAO, *Report to Congressional Requesters*, at 29 (June 2007), http://www.gao.gov/new.items/d07737.pdf (last visited Nov. 26, 2024).

H. Plaintiff and Class Members Suffered Damages.

87. As a direct and proximate result of VPS's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have already been harmed by the fraudulent misuse of their Private Information, and have been placed at an imminent, immediate, and continuing increased risk of additional harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate both the actual and potential impact of the Data Breach on their lives. Such mitigatory actions include, *inter alia*, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, sorting through dozens of phishing and spam email, text, and phone communications, and filing police reports. This time has been lost forever and cannot be recaptured.

88. VPS's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Private Information, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft and misuse of their personal and financial information;

b. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

c. the untimely and inadequate notification of the Data Breach;

d. the improper disclosure of their Private Information;

e. loss of privacy;

f. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

g. ascertainable losses in the form of deprivation of the value of their Private Information, for which there is a well-established national and international market;

h. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience,

nuisance and annoyance of dealing with all such issues resulting from the Data Breach; and

i. nominal damages.

89. While Plaintiff's and Class Members' Private Information has been stolen, VPS continues to hold Plaintiff's and Class Members' Private Information. Particularly because VPS have demonstrated an inability to prevent a breach or stop it from continuing even after being detected, Plaintiff and Class Members have an undeniable interest in ensuring that their Private Information is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

I. Plaintiff's Experience.

90. Upon information and belief, Defendant obtained Plaintiff's Private Information in the course of conducting its regular business operations.

91. Upon information and belief, at the time of the Data Breach, Defendant maintained Plaintiff's Private Information in its system.

92. Plaintiff received a Notice Letter from VPS concerning the Data Breach dated November 15, 2024, which informed him that his Private Information had been compromised in the Data Breach.

93. Since the Data Breach, Plaintiff has experienced anxiety and increased concerns for the loss of his privacy, as well as anxiety over the impact of cybercriminals accessing and using his Private Information.

94. Plaintiff would not have entrusted his Private Information to VPS had he known VPS would not take reasonable steps to safeguard his information.

95. Plaintiff is very careful about sharing sensitive Private Information. He stores documents containing Private Information in safe and secure locations and has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Plaintiff would not have entrusted his Private Information to VPS had he known of VPS's lax data security policies.

96. As a result of the Data Breach, Plaintiff made reasonable efforts to mitigate the impact of the Data Breach, including researching and verifying the legitimacy of the Data Breach. Plaintiff has spent significant time dealing with the Data Breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

97. Plaintiff suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his Private Information, a form of property that Defendant obtained from Plaintiff; (b) violation of him privacy rights; (c) the theft of his Private Information; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

98. As a result of the Data Breach, Plaintiff is very concerned about identity

theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

99. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed him of key details about the Data Breach's occurrence.

100. As a result of the Data Breach, Plaintiff anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff will continue to be at present, imminent, and continued increased risk of identity theft and fraud for him lifetime.

101. Plaintiff has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

102. Plaintiff brings this class action individually on behalf of himself and on behalf of all members of the following Class of similarly situated persons. Plaintiff seeks certification of the following Class:

> All persons residing in the United States whose Private Information was compromised in the Data Breach, including all who were sent a notice of the Data Breach.

103. Excluded from the Class are VPS and its affiliates, parents, subsidiaries, officers, agents, and directors, any entities in which VPS has a controlling interest,

as well as the judge(s) presiding over this matter and the clerks, judicial staff, and immediate family members of said judge(s).

104. Plaintiff reserves the right to modify or amend the foregoing Class definitions before the Court determines whether certification is appropriate.

105. Numerosity: The members in the Class are so numerous that joinder of all Class Members in a single proceeding would be impracticable. The exact number of Class Members is unknown to Plaintiff now.

106. Commonality and Predominance: Common questions of law and fact exist as to all Class Members and predominate over any potential questions affecting only individual Class Members. These common questions of law or fact include, *inter alia*:

a. Whether VPS engaged in the conduct alleged herein;

b. Whether VPS had a duty to implement and maintain reasonable security procedures and practices to protect and secure Plaintiff's and Class Members' Private Information from unauthorized access and disclosure;

c. Whether VPS's computer systems and data security practices used to protect Plaintiff's and Class Members' Private Information violated the FTC Act and/or state laws, and/or VPS other duties discussed herein;

d. Whether VPS failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and Class Members;

e. Whether VPS unlawfully shared, lost, or disclosed Plaintiff's and Class Members' Private Information;

f. Whether VPS's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

g. Whether VPS's data security systems prior to and during the Data Breach were consistent with industry standards;

h. Whether Plaintiff and Class Members suffered injury as a proximate result of VPS's negligent actions or failures to act;

i. Whether VPS's failed to exercise reasonable care to secure and safeguard Plaintiff's and Class Members' Private Information;

j. Whether VPS breached duties to protect Plaintiff's and Class Members' Private Information;

k. Whether VPS's actions and inactions alleged herein were negligent;

l. Whether VPS were unjustly enriched by their conduct as alleged herein;

m. Whether an implied contract existed between Class Members and VPS with respect to protecting Private Information and privacy, and whether that contract was breached;

n. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages or other relief, and the measure of such damages and relief;

o. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

p. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

107. VPS engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff on behalf of himself and all other Class Members. Individual questions, if any, pale in comparison, in both quantity and quality, to the numerous common questions that dominate this action.

108. Typicality: Plaintiff's claims are typical of the claims of the Class. Plaintiff, like all proposed members of the Class, had his Private Information compromised in the Data Breach. Plaintiff and Class Members were injured by the

same wrongful acts, practices, and omissions committed by VPS, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that give rise to the claims of all Class Members.

109. Adequacy: Plaintiff will fairly and adequately protect the interests of the Class Members. Plaintiff is an adequate representative of the Class and has no interests adverse to, or conflict with, the Class he seeks to represent. Plaintiff has retained counsel with substantial experience and success in the prosecution of complex consumer protection class actions of this nature.

110. Superiority: A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages and other financial detriment suffered by Plaintiff and all other Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against VPS, so it would be impracticable for Class Members to individually seek redress from VPS's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and

provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

111. Injunctive and Declaratory Relief: VPS has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

112. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this mater and the parties' interests therein. Such issues include, but are not limited to: (a) whether VPS owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Private Information; (b) whether VPS failed to adequately monitor and audit their data security systems; and (c) whether VPS failed to take reasonable steps to safeguard the Private Information of Plaintiff and Class Members.

113. All members of the proposed Class are readily ascertainable. VPS has access to the names in combination with addresses and/or e-mail addresses of Class Members affected by the Data Breach. Indeed, impacted Class Members already have been preliminarily identified and sent a breach notice letter.

CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Class)

114. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

115. VPS's require their patients to submit non-public Private Information as a condition of obtaining healthcare services.

116. VPS gathered and stored the Private Information of Plaintiff and Class Members as part of its business, which affects commerce.

117. Plaintiff and Class Members entrusted VPS with their Private Information with the understanding that the information would be safeguarded.

118. VPS had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and Class Members could and would suffer if their Private Information were wrongfully disclosed.

119. By assuming the responsibility to collect and store this data, VPS had duties of care to use reasonable means to secure and to prevent disclosure of the information, and to safeguard the information from theft.

120. VPS owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein,

and to ensure that their systems and networks, and the personnel responsible for them, adequately protected the Private Information.

121. VPS's duty to use reasonable security measures arose as a result of the special relationship that existed between VPS, on the one hand, and Plaintiff and Class Members, on the other hand. That special relationship arose because VPS was entrusted with their confidential Private Information, a necessary part of healthcare services.

122. VPS also had a duty to exercise appropriate clearinghouse practices to remove former patients' Private Information they were no longer required to retain pursuant to regulations.

123. Moreover, VPS had a duty to promptly and adequately notify Plaintiff and the Class of the Data Breach, but failed to do so.

124. VPS had and continues to have duties to adequately disclose that Plaintiff's and Class Members' Private Information within VPS's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

125. VPS breached its duties and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information.

The specific negligent acts and omissions committed by VPS include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of their networks and systems;

c. Allowing unauthorized access to Class Members' Private Information;

d. Failing to detect in a timely manner that Class Members' Private Information had been compromised;

e. Failing to remove former patients' Private Information they were no longer required to retain pursuant to regulations; and

f. Failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

126. VPS breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

127. VPS knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

128. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

129. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of VPS's inadequate security practices.

130. It was foreseeable that VPS's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of corporate cyberattacks and data breaches.

131. VPS had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiff and the Class could and would suffer if the Private Information were wrongfully disclosed.

132. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. VPS knew or should have known of the inherent risks in collecting and storing Private Information, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information stored on its systems.

133. Plaintiff and the Class had no ability to protect their Private Information that was in, and possibly remains in, VPS's possession.

134. VPS was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

135. VPS's duties extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which have been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

136. VPS has admitted that the Private Information of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

137. But for VPS's wrongful and negligent breaches of duties owed to Plaintiff and the Class, Plaintiff's and Class Members' Private Information would not have been compromised.

138. There is a close causal connection between VPS's failure to implement security measures to protect Plaintiff's and Class Members' Private Information, and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. Private

Information was lost and accessed as the proximate result of VPS's failure to exercise reasonable care by adopting, implementing, and maintaining appropriate security measures.

139. As a direct and proximate result of VPS's negligence, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in VPS's possession and is subject to further unauthorized disclosures so long as VPS fails to undertake appropriate and adequate measures to protect the Private Information; (viii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PII/PHI for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by VPS's data breach; (x) the value of the unauthorized access to their PII/PHI permitted by Defendant; and (xi) any nominal damages that may be awarded.

140. As a direct and proximate result of VPS's negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses including nominal damages.

141. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

142. VPS's negligent conduct is ongoing, in that it still possesses Plaintiff's and Class Members' Private Information in an unsafe and insecure manner.

143. Plaintiff and Class Members are entitled to injunctive relief requiring VPS to: (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

144. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

145. VPS had duties arising under HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and the FTC Act to protect Plaintiff's and Class Members' Private Information.

146. VPS breached its duties, pursuant to the FTC Act and other applicable standards, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' Private Information. The specific negligent acts and omissions committed by VPS include, but are not limited to, the following: (i) failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information; (ii) failing to adequately monitor the security of their networks and systems; (iii) allowing unauthorized access to Class Members' Private Information; (iv) failing to detect in a timely manner that Class Members' Private Information had been compromised; (v) failing to remove former patients' Private Information they were no longer required to retain pursuant to regulations; and (vi) failing to timely and adequately notify Class Members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

147. VPS's violation of HIPAA, the HIPAA Privacy Rule and Security Rule, HITECH, and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

148. Plaintiff and Class Members are consumers within the class of persons that HIPAA, HITECH, and Section 5 of the FTC Act were intended to protect.

149. The harm that has occurred is the type of harm HIPAA, HITECH, and the FTC Act were intended to guard against.

150. The FTC has pursued enforcement actions against businesses and healthcare entities that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

151. VPS breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

152. In addition, under state data security and consumer protection statutes such as those outlined herein, VPS had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Private Information.

153. Plaintiff and Class Members were foreseeable victims of VPS's violations of HIPAA, HITECH, and the FTC Act, and state data security and consumer protection statutes. VPS knew or should have known that its failure to implement reasonable data security measures to protect and safeguard Plaintiff's and Class Members' Private Information would cause damage to Plaintiff and the Class.

154. As a direct and proximate result of VPS's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity

costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in VPS's possession and is subject to further unauthorized disclosures so long as VPS fails to undertake appropriate and adequate measures to protect the Private Information.

155. As a direct and proximate result of VPS's negligence per se Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

156. Finally, as a direct and proximate result of VPS's negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remain in VPS's possession and is subject to further unauthorized disclosures so long as VPS fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

157. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

158. When Plaintiff and Class Members provided their Private Information to Defendant VPS in exchange for Defendant VPS's services, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

159. VPS solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

160. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and adhered to industry standards.

161. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

162. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

163. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of their implied promise to monitor their

computer systems and networks to ensure that it adopted reasonable data security measures.

164. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

165. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

166. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

167. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

168. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Class)

169. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

170. This count is pleaded in the alternative to the breach of implied contract claim above against VPS (Count III).

171. Plaintiff and Class Members conferred a monetary benefit on VPS in connection with obtaining healthcare services, specifically providing VPS, through their healthcare providers, with their Private Information.

172. VPS knew that Plaintiff and Class Members conferred a benefit upon it and accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. VPS profited from Plaintiff's retained data and use Plaintiff's and Class Members' Private Information for business purposes.

173. VPS failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

174. VPS acquired the Private Information through inequitable record retention as it failed to disclose the inadequate vendor vetting and data security practices previously alleged.

175. Under the circumstances, it would be unjust for VPS to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

176. As a direct an proximate result of VPS's conduct, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) the actual misuse of their compromised Private Information; (ii) invasion of privacy; (iii) lost or

diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) an increase in spam calls, texts, and/or emails; (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in VPS's possession and is subject to further unauthorized disclosures or further entrustment to inadequate third party vendors so long as VPS fails to undertake appropriate and adequate measures to protect the Private Information; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised Private Information for the rest of their lives; (ix) the present value of ongoing credit monitoring and identity defense services necessitated by VPS's data breach; (x) the value of the unauthorized access to their Private Information permitted by Defendant; and (xi) any nominal damages that may be awarded.

177. Plaintiff and Class Members are entitled to restitution and/or damages from VPS and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by VPS from its wrongful conduct, as well as return of their sensitive Private Information and/or confirmation that it is secure. This can be accomplished by establishing a constructive trust from which the Plaintiff and Class

Members may seek restitution or compensation.

178. Plaintiff and Class Members may not have an adequate remedy at law against VPS, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

179. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

180. Defendant became guardian of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant VPS and Plaintiff and Class Members.

181. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

182. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of VPS's relationship with its patients, in particular, to keep secure their Private Information.

183. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

184. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

185. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

186. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching

how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in their continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

187. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
DECLARATORY JUDGEMENT
(On Behalf of Plaintiff and the Class)

188. Plaintiff restates and realleges the foregoing paragraphs as if fully set forth herein.

189. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority

to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

190. Defendant owes a duty of care to Plaintiff and Class Members which required it to adequately secure Private Information.

191. Defendant still possesses Private Information regarding Plaintiff and Class Members.

192. Plaintiff alleges that Defendant's data security measures remain inadequate. Furthermore, Plaintiff continues to suffer injury as a result of the compromise of Private Information, and remains at imminent risk that further compromises of the Private Information will occur in the future.

193. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant owes a legal duty to secure patients' Private Information and to timely notify patients of a data breach under the common law and Section 5 of the FTCA;

b. Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect patients' Private Information; and

c. Defendant continues to breach this legal duty by failing to employ

reasonable measures to secure patients' Private Information.

194. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry standards to protect patients' Private Information, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members, and

b. Order Defendant to comply with its explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures.

195. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

196. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by finally employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

197. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiff and patients whose Private Information would be further compromised.

PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all other members of the class, respectfully requests that the Court enter judgment in Plaintiff's favor and against VPS as follows:

A. Certifying the Class as requested herein, designating Plaintiff as Class representatives, and appointing Plaintiff's counsel as Class Counsel;

B. Awarding Plaintiff and the Class appropriate monetary relief, including actual damages, statutory damages, punitive damages, restitution, nominal damages and disgorgement;

C. Awarding Plaintiff and the Class equitable, injunctive, and declaratory relief, as may be appropriate. Plaintiff, on behalf of himself and the class, seek appropriate injunctive relief designed to prevent VPS from experiencing another data breach by adopting and implementing best data security practices to safeguard PII and to provide or extend credit monitoring services and similar services to protect against all types of identity theft;

D. Awarding Plaintiff and the Class pre-judgment and post-judgment interest to the maximum extent allowable;

E. Awarding Plaintiff and the Class reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Awarding Plaintiff and the Class such other favorable relief as allowable under law.

JURY TRIAL DEMAND

Plaintiff demands a trial by jury of all claims in this Class Action Complaint so triable.

Dated: December 3, 2024.

Respectfully submitted,

/s/ E. Powell Miller
E. Powell Miller (P39487)
Emily E. Hughes (P68724)
THE MILLER LAW FIRM, P.C.
950 W. University Dr., Suite 300
Rochester, MI 48307
T: (248) 841-2200
epm@millerlawpc.com
eeh@millerlawpc.com

Gary M. Klinger (*admission forthcoming)*
MILBERG COLEMAN BRYSON
PHILLIPS GROSSMAN PLLC
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Phone: (866) 252-0878
gklinger@milberg.com

Counsel for Plaintiff and the Proposed Class